1. (Currently Amended) A method for securing software to reduce unauthorized use of the software, the method comprising:

providing software including data representing digital content;

associating at least one identifier with the software prior to distribution of the software, the identifier being detectable ~~by an authorized representative~~ to request authentication of the software by an authorized representative, but allowing the software to function if not detected; and

distributing the software with the at least one identifier to a user.

2. (Original) The method of claim 1 wherein the software is self activating and self authenticating in conjunction with an authorized representative located on or in the user device.

3. (Original) The method of claim 1 wherein the digital content is selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.

4. (Original) The method of claim 1 wherein the identifier is hidden from the user.

5. (Original) The method of claim 1 wherein the identifier is tamper resistant to the user.

6. (Original) The method of claim 1 wherein the at least one identifier is embedded within a file of at least one component of the software.

7. (Original) The method of claim 1 wherein the at least one identifier is a binary code.

8. (Original) The method of claim 1 wherein the at least one identifier is encrypted.

9. (Original) The method of claim 1 wherein the step of distributing the software comprises electronically distributing the software.

10. (Original) The method of claim 1 wherein the step of distributing the software comprises distributing the software on a computer readable storage medium.

11. (Original) The method of claim 1 further comprising:

performing a process to determine whether an attempted access to the software is authorized based on detection of the at least one identifier.

12. (Original) The method of claim 11 wherein the step of performing a process comprises:

determining whether the attempted access to the software is authorized based on registration information associated with the software.

13. (Original) The method of claim 11 wherein the step of performing a process comprises:

determining whether the attempted access to the software is authorized based on registration information associated with the software and registration information associated with a user device.

14. (Original) The method of claim 1 further comprising:

communicating registration information to an authorized representative of the software;

generating at least one authentication code based on the registration information; and

associating the authentication code with the software.

15. (Original) The method of claim 14 wherein authorized representative functions are implemented by a user device.

16. (Original) The method of claim 14 wherein authorized representative functions are implemented by software.

17. (Original) The method of claim 14 wherein authorized representative functions are implemented by hardware.

18. (Original) The method of claim 14 wherein authorized representative functions are implemented by hardware and software.

19. (Original) The method of claim 1 wherein the at least one identifier is included in a filename for at least one component of the software.

20. (Original) The method of claim 19 wherein the identifier is selected from the group consisting of the filename, a filename prefix, a filename suffix, a filename extension, a filename extension prefix, and a filename extension suffix.

21. (Original) The method of claim 19 wherein the identifier is tamper resistant to the user.

22. (Original) The method of claim 19 wherein the identifier is hidden to the user.

23. (Currently Amended) A method for securing software to reduce unauthorized use of the software, the method comprising:

providing software including data representing digital content;

associating a plurality of identifiers with the software prior to distribution of the software, at least one identifier being detectable by an authorized representative to request authentication of the software without requiring contact with a remote authorized representative; and

distributing the software with the plurality of identifiers to a user.

24. (Original) The method of claim 23 wherein the software is self activating and self authenticating in conjunction with an authorized representative located on or in the user device.

25. (Original) The method of claim 23 wherein at least one of the identifiers is an activation code that must be entered by the user prior to transferring the software.

26. (Original) The method of claim 23 wherein the digital content is selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.

27. (Original) The method of claim 23 wherein at least one of the at least one identifiers is hidden from the user.

28. (Original) The method of claim 23 wherein at least one of the at least one identifiers is tamper resistant to the user.

29. (Original) The method of claim 23 wherein the at least one identifier is embedded within a file of at least one component of the software.

30. (Original) The method of claim 23 wherein the at least one identifier is a binary code.

31. (Original) The method of claim 23 wherein the at least one identifier is encrypted.

32. (Original) The method of claim 23 wherein the step of distributing the software comprises electronically distributing the software.

33. (Original) The method of claim 23 wherein the step of distributing the software comprises distributing the software on a computer readable storage medium.

34. (Original) The method of claim 23 further comprising:

performing a process to determine whether an attempted access to the software is authorized based on detection of the at least one identifier.

35. (Original) The method of claim 34 wherein the step of performing a process comprises:

determining whether the attempted access to the software is authorized based on registration information associated with the software.

36. (Original) The method of claim 34 wherein the step of performing a process comprises:

determining whether the attempted access to the software is authorized based on registration information associated with the software and registration information associated with a user device.

37. (Original) The method of claim 23 further comprising:

communicating registration information to an authorized representative of the software;

generating at least one authentication code based on the registration information; and

associating the authentication code with the software.

38. (Original) The method of claim 37 wherein authorized representative functions are implemented by a user device.

39. (Original) The method of claim 37 wherein authorized representative functions are implemented by software.

40. (Original) The method of claim 37 wherein authorized representative functions are implemented by hardware.

41. (Original) The method of claim 37 wherein authorized representative functions are implemented by hardware and software.

42. (Original) The method of claim 23 wherein the at least one identifier is included in a file name for at least one component of the software.

43. (Original) The method of claim 42 wherein the identifier is selected from the group consisting of a filename, a filename prefix, a filename suffix, a filename extension, a filename extension prefix, and a filename extension suffix.

44. (Original) The method of claim 42 wherein the identifier is tamper resistant to the user.

45. (Original) The method of claim 42 wherein the identifier is hidden to the user.

46. (Currently Amended) A method for securing software to reduce unauthorized use having at least one authorized representative entity installed on or in a user device, the method comprising:

associating at least one identifier with the software to designate the software for protection from unauthorized use;

detecting the at least one identifier using the authorized representative installed on or in the user device;

determining whether the user device is authorized to access the software using the authorized representative entity installed on or in the user device without requiring contact with a remote authorized representative entity; and

controlling access to the software based on whether the user device is determined to be authorized.

47. (Original) The method of claim 46 wherein the software is self activating and self authenticating in conjunction with an authorized representative located on or in the user device.

48. (Original) The method of claim 46 further comprising:

determining whether the user device is authorized to access the software using a remotely located authorized representative entity in combination with the at least one authorized representative entity installed on or in the user device.

49. (Original) The method of claim 46 wherein the at least one authorized representative entity installed on or in the user device comprises a computer chip.

50. (Original) The method of claim 46 wherein the at least one authorized representative entity installed on or in the user device comprises program instructions executed by a microprocessor.

51. (Original) The method of claim 50 wherein the program instructions comprise an operating system component.

52. (Original) The method of claim 50 wherein the program instructions comprise an application program.

53. (Original) The method of claim 50 wherein the program instructions comprise a driver for a secondary device.

54. (Original) The method of claim 46 wherein the step of determining whether the user device is authorized comprises:

comparing registration information associated with the user device to registration information associated with the software.

55. (Original) The method of claim 54 wherein the registration information associated with the software is embedded within an authentication code.

56. (Original) The method of claim 54 wherein the registration information associated with the software is encrypted.

57. (Original) The method of claim 54 wherein the registration information includes hardware information.

58. (Original) The method of claim 57 wherein the registration information includes hardware information associated with a unique user device.

59. (Original) The method of claim 57 wherein the hardware information includes a serial number.

60. (Original) The method of claim 57 wherein the registration information includes hardware information associated with a group of user devices.

61. (Original) The method of claim 46 wherein the authorized representative entity is installed by a manufacturer of the user device.

62. (Original) The method of claim 46 wherein the authorized representative entity is installed from a computer readable storage medium.

63. (Original) The method of claim 46 wherein the authorized representative entity is installed from the software.

64. (Original) The method of claim 46 wherein the authorized representative entity is downloaded to the user device.

65. (Original) The method of claim 46 wherein the authorized representative entity is transferred to the user device from a network.

66. (Original) The method of claim 46 wherein the step of controlling access comprises preventing the software from being transferred to a second user device.

67. (Original) The method of claim 46 wherein the step of controlling access comprises preventing the software from being transferred to a user device if at least one authorized representative is inaccessible.

68. (Original) The method of claim 46 wherein the step of controlling access comprises preventing the software from being installed on a user device if at least one authorized representative is not present.

69. (Original) The method of claim 46 wherein the step of controlling access comprises preventing the software from being executed by the user device.

70. (Original) The method of claim 46 wherein the step of controlling access comprises providing limited access to the software.

71. (Original) The method of claim 46 wherein the software comprises digital content.

72. (Original) The method of claim 71 wherein the software is selected from the group consisting of data representing music, data representing video, instructions executable by a computer, code for an application program, code for an operating system, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.

73. (Original) The method of claim 46 wherein the software comprises instructions for generating at least one authentication code based on registration information associated with the user device.

74. (Original) The method of claim 73 wherein the software comprises instructions for encrypting the authentication code.

75. (Currently Amended) A method for securing software to reduce unauthorized use of the software, the method comprising:

providing software including data representing digital content;

detecting an identifier associated with the software indicating that protection from unauthorized use is desired;

communicating with an authorized representative entity to determine whether a user device attempting to access the software is authorized to access the software; and

controlling access to the software based on whether the user device is authorized without requiring continuous communication with a remote authorized representative entity.

76. (Original) The method of claim 75 wherein the software is self activating and self authenticating in conjunction with an authorized representative located on or in the user device.

77. (Original) The method of claim 75 wherein the identifier associated with the software is contained within a filename for the software.

78. (Original) The method of claim 75 wherein the authorized representative entity is a hardware device.

79. (Original) The method of claim 75 wherein the step of communicating with the authorized representative entity comprises communicating with at least one software module associated with the user device.

80. (Original) The method of claim 75 wherein the authorized representative entity is installed on the user device.

81. (Original) The method of claim 75 further comprising:

generating an authentication code based on registration information associated with the user device; and

associating the authentication code with the software.

82. (Original) The method of claim 75 wherein the step of communicating comprises:

generating an authentication code based on registration information associated with the user device; and

comparing the authentication code with a previously generated authentication code associated with the software to determine if the user device is authorized.

83. (Original) The method of claim 82 wherein the step of comparing the authentication code comprises determining if at least a portion of system information associated with the user device matches system information encoded within the authentication code associated with the software.

84. (Original) The method of claim 81 wherein the registration information includes hardware-specific information.

85. (Original) The method of claim 75 wherein the authorized representative entity is installed on or in the user device.

86. (Original) The method of claim 75 wherein the digital content is selected from the group consisting of data representing music, data representing video,

instructions executable by a computer, code for an application program, code for an operating system, code for a game, data representing a movie, data representing graphics, data representing watermarked works, data representing a magazine, and data representing a book.